(ii) creating a second signature comprising a plurality of parameters related to the transmission of messages over a second period shorter than the first and more recent than the first;

(iii) updating the first signature by a weighted averaging with the second signature; [and]

(iv) [deriving said anomalies by providing said signatures as input to an anomaly detector] inputting the signatures to the anomaly detector; and

(v) processing the signatures using the anomaly detector to derive the anomalies by detecting unexpected patterns in the transmission of messages by the entity over the time period.

8. (twice amended) A method as claimed in Claim 1 wherein said anomaly detector [step (iv) of deriving anomalies] comprises [providing said signatures as input to] a neural network.

10. (twice amended) The method of Claim 1 wherein said step [(iv)] (v) of [deriving anomalies] processing the signatures is carried out using a predictive model, the method further comprising the steps of:

monitoring the performance of the model; and

automatically updating the model when the performance reaches a predetermined threshold.

11. (twice amended) The method of Claim 1 wherein said step [(iv)] (v) of [deriving anomalies] processing the signatures is carried out using a predictive model, and wherein the model is implemented using at least one instantiated object created using an object oriented programming language and the method further comprises the steps of:

converting the object into a data structure;

storing the data structure; and

recreating the object from the data structure.

12. (twice amended) A computer system for detecting anomalies in the transmission of messages by an entity by storing information relating to the transmission of messages by the entity over a given time period, said computer system comprising:

(i) an input arranged to receive information about each of a number of events which occurred during the time period;

(ii) a processor arranged to convert the information into a signature comprising a plurality of parameters related to the transmission of messages over the time period wherein the parameters comprise at least one parameter related to the transmission of messages over a portion of the period and also related to the position of the portion in the period, to enable output data to be derived from the stored information and wherein said processor is further arranged to convert at least part of the information into a second signature, comprising a plurality of parameters related to the transmission of messages over a second period, shorter than the first and more recent than the first; and also to update the first signature by a weighted averaging with the second signature; [and]

(iii) [an input arranged to provide said signatures to an anomaly detector to derive said anomalies] an anomaly detector;

(iv) an input arranged to provide the signatures to the anomaly detector; and

(v) wherein the anomaly detector is arranged to process the signatures to derive the anomalies by detecting unexpected patterns in the transmission of messages by the entity over the time period.

13. (twice amended) A method of deriving anomalies from information relating to the transmission of messages by an entity over time, using an anomaly detector and comprising the steps of:

(i) creating a first signature comprising a plurality of parameters related to the transmission of messages over a predetermined first time period;

(ii) creating a second signature comprising a plurality of parameters related to the transmission of messages over a second period shorter than the first and more recent than the first;

(iii) updating the first signature by a weighted averaging with the second signature;

[and] (iv) [deriving said anomalies using the signatures] inputting the signatures to the anomaly detector; and

(v) processing the signatures using the anomaly detector to derive the anomalies by detecting unexpected patterns in the transmission of messages by the entity over the time period.

20. (once amended) A method as claimed in claim 13 wherein the [data deriving step] step of processing the signatures is carried out using a predictive model, the method further comprising the steps of:

monitoring the performance of the model; and

automatically updating the model when the performance reaches a predetermined threshold.

21. (twice amended) The method of Claim 13 wherein said step [(iv)] (v) of [deriving said anomalies] processing the signatures is carried out using a predictive model, and wherein the model is implemented using at least one instantiated object created using an object oriented programming language and the method further comprises the steps of;

converting the object into a data structure;

storing the data structure; and

recreating the object from the data structure.

22. (twice amended) A computer system for deriving anomalies from information relating to the transmission of messages by an entity over time, the system comprising:

an input arranged to receive information about the transmission of messages by the entity;

a processor arranged to create a first signature comprising a plurality of parameters related to the transmission of messages over a predetermined first time period and to create a second signature